(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－48478
(P2000－48478A)
(43)公開日　平成12年２月18日(2000.2.18)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

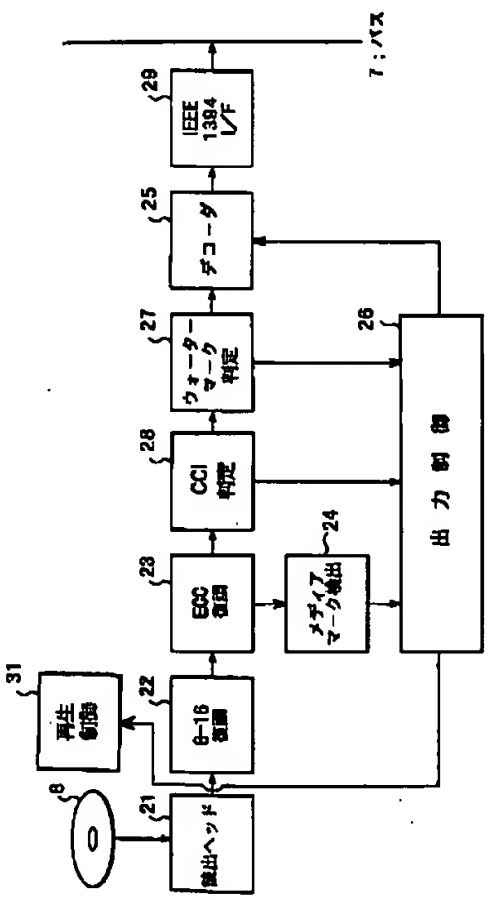
(21)出願番号　特願平10－192084
(22)出願日　平成10年７月７日(1998.7.7)
(31)優先権主張番号　特願平10－161361
(32)優先日　平成10年５月26日(1998.5.26)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000004075
ヤマハ株式会社
静岡県浜松市中沢町10番１号
(72)発明者　松本　誠二
静岡県浜松市中沢町10番１号　ヤマハ株式会社内
(72)発明者　古川　雅通
静岡県浜松市中沢町10番１号　ヤマハ株式会社内
(74)代理人　100092820
弁理士　伊丹　勝

Ｆターム(参考)　5D044 AB05 AB07 BC01 BC02 CC03
CC04 DE50 DE68 EF05 FG18
GK17 HL08 HL11

(54)【発明の名称】　ディジタルコピー制御方法及びそれを用いた装置

(57)【要約】
【課題】　コピーを制限する態様を可能にしつつ、許可されないディジタルコピーをより効果的に防止する。
【解決手段】　３種類の情報によってディジタル記録媒体の正当性を判定する。第１の情報は、メインデータの映像・音声以外の部分に含まれるコピー制限レベルを示すコピー管理情報で、ディジタルコピーを制限する場合、コピーされるとコピー制限レベルが強化されるように書き替えられる。第２の情報は、同じくメインデータの映像・音声の部分に含まれてコピー制限レベルを示す電子透かし情報で、この情報はディジタルコピーされても書き替えられないし、書き換えは極めて困難である。第３の情報は、エラー訂正後のデータに意図的に付加される特定パターンのエラー情報（媒体マーク）で、この情報は、メインデータ外に付加されるものであるから、記録媒体から再生されたメインデータには含まれず、ディジタルコピーされると消失する。



【特許請求の範囲】
【請求項１】　バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器および受信側機器は、前記ディジタルデータに含まれるコピー制限のためのコピー管理情報の内容に基づいて不許可コピーを防止するように、当該送信側機器および受信側機器の再生および記録動作の動作制限を行うディジタルコピー制御方法において、
前記ディジタル記録媒体に記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示す前記コピー管理情報を付加し、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報を付加すると共に、前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報を意図的に付加し、
前記送信側機器で再生されるディジタル記録媒体の正当性を、前記コピー管理情報、電子透かし情報、及び特定パターンのエラー情報の有無により識別して、正当なディジタル記録媒体のデータのみその再生を行い、また適切なデータのみ記録することを特徴とするディジタルコピー制御方法。
【請求項２】　再生または別途記録するためにメインデータが記録されてなるディジタル記録媒体において、
前記メインデータには、映像及び／又は音声以外の部分にコピー制限レベルを示すとともにディジタルコピーを制限する場合ディジタルコピーによって前記コピー制限レベルを強化するように書き替えられるコピー管理情報が含まれ、また、映像及び／又は音声以外の部分にはディジタルコピーによっても書き替えられない電子透かし情報とが外部に読み出し可能な状態で含まれ、
前記メインデータ外には、外部に読み出されない媒体マークが付加され、
これらコピー管理情報、電子透かし情報、および媒体マークは、これら３種類の情報の内容の組み合わせによって前記メインデータの作成者側の意図するところの、媒体再生管理および媒体コピー管理がなされるように構成されていることを特徴とするディジタル記録媒体。
【請求項３】　原データにその特徴を損なわない電子透かし情報を付加する透かし情報付加手段と、
原データにコピーを制限するためのコピー管理情報を付加するコピー管理情報付加手段と、
原データに前記電子透かし情報及びコピー管理情報が付加されたメインデータからエラー訂正コードを生成して付加するエラー訂正コード生成手段と、
このエラー訂正コード生成手段でエラー訂正コードが付加されたデータに特定パターンのエラーを媒体マークとして付加するエラー付加手段とを備えたことを特徴とするディジタル記録媒体作製装置。
【請求項４】　バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記送信側機器として用いられるディジタル再生装置において、
ディジタル記録媒体から記録データを読み出す読出手段と、
この読出手段で読み出された読出データからエラー訂正コードを抽出し、このエラー訂正コードに基づいて読出データの誤りを検出訂正する誤り検出訂正手段と、
この誤り検出訂正手段で検出された誤りが特定パターンであることを検出する特定パターン誤り検出手段と、
前記誤り検出訂正手段で誤り訂正されたデータを前記インタフェースの仕様に合ったディジタル情報の形態で前記バスに出力する出力手段と、
前記誤り訂正されたデータに含まれるディジタルコピーを制限するためのコピー管理情報を識別して判定するコピー管理情報判定手段と、
前記誤り訂正されたデータからコピー制限レベルを示す電子透かし情報を識別して判定する電子透かし情報判定手段とを備え、
前記特定パターン誤り検出手段の検出結果に基づいて前記ディジタル記録媒体がオリジナル媒体かコピー媒体かを判定し、この判定結果と、前記コピー管理情報判定手段及び前記電子透かし情報判定手段での判定結果とに基づいて前記送信側機器のデータの再生を許可又は禁止するようにしたことを特徴とするディジタル再生装置。
【請求項５】　前記コピー管理情報判定手段は、前記コピー管理情報からコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルを識別し、
前記電子透かし情報判定手段は、前記電子透かし情報からコピーフリー又はコピー禁止の２種類のコピー制限レベルを識別し、
前記特定パターン誤り検出手段は、前記特定パターンの誤りの有無を識別し、
これら各手段での識別結果から正規に記録されたディスクであるかどうかを判定して正規のディスクのみ再生するようにしたことを特徴とする請求項４記載のディジタル再生装置。
【請求項６】　前記特定パターン誤り検出手段で特定パターンの誤りが検出され、コピー管理情報判定手段で１世代コピー可と判定され、且つ電子透かし情報判定手段で電子透かし情報がコピー禁止であると判定された場合、再生動作を実行することを特徴とする請求項５記載のディジタル再生装置。
【請求項７】　前記特定パターン誤り検出手段で特定パターンの誤りが検出された場合で且つ前記コピー管理情

報判定手段と前記電子透かし情報判定手段の判定結果が、コピー管理情報が１世代コピー可で且つ電子透かし情報がコピー禁止となっている場合を除いて相矛盾する内容となっているとき、又は前記特定パターンの誤り検出手段で特定パターンの誤りが検出された場合で且つ前記電子透かし情報が検出出来なかった場合、再生を行わないことを特徴とする請求項４又は５記載のディジタル再生装置。

【請求項８】　前記特定パターンの誤り検出手段で特定パターンの誤りが検出されなかった場合で且つ、前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が異なる場合、再生を行わないことを特徴とする請求項４又は５記載のディジタル再生装置。

【請求項９】　バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記受信側機器として用いられるディジタル記録装置において、

映像及び／又は音声以外の部分にコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルを示す前記コピー管理情報が付加されると共に、映像及び／又は音声の部分にコピー可又はコピー禁止の２種類の電子透かし情報が付加されたディジタルデータを受信する受信し、

識別されたコピー管理情報が１世代コピー可で、且つ識別された電子透かし情報がコピー禁止である場合、電子透かし情報はそのまま記録し、コピー管理情報のみコピー禁止に書き換えて記録することを特徴とするディジタル記録装置。

【請求項１０】前記認証された機器には、ディジタル記録媒体に記録されたディジタルデータコンテンツを前記インターフェースを介することなくアナログ信号として出力可能に構成された機器、及びアナログ信号で入力されるデータコンテンツを前記インターフェースを介することなく新たなディジタル記録媒体に記録可能に構成された機器を含み、これら認証された機器の全ては、アナログ信号またはディジタル信号で供給されるデータコンテンツをディジタル記録媒体にディジタル記録する際に、当該媒体上にデータコンテンツに加えて当該認証された機器間でのみ認証可能な電子認証署名データを記録するように構成されると共に、

ディジタル記録媒体に記録されたディジタルデータコンテンツを再生する際に、当該媒体上に前記認証された機器間でのみ認証可能な電子認証署名データが存在するか否かを検出し、

認証された場合のみ当該媒体のディジタルデータコンテンツを再生するように制御されることを特徴とする請求項１記載のディジタルコピー制御方法。

【請求項１１】認証された機器間でのみ認証可能な電子認証署名データが、更に記録されてなることを特徴とする請求項２記載のディジタル記録媒体。

【請求項１２】認証された機器間でのみ認証可能な電子認証署名データを検出する手段と、電子認証署名データが認証されなかった場合はデータの再生を禁止する手段とを、更に有することを特徴とする請求項４記載のディジタル再生装置。

【請求項１３】前記認証された機器の少なくとも一部は、ディジタル記録媒体に記録されたディジタルデータコンテンツを前記インターフェースを介することなくアナログ信号として出力可能に構成されており、

これらアナログ信号で供給されるデータコンテンツをディジタル記録媒体にディジタル記録する際に、データコンテンツに加え当該認証された機器間でのみ認証可能な電子認証署名データを当該媒体上に記録するように構成されることを特徴とする請求項９記載のディジタル記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ＤＶＤ（ディジタル・ビデオ・ディスク）記録再生装置、ディジタルＶＴＲ、ディジタルＴＶ等のディジタル機器が相互認証機能を備えたインタフェースを介して接続されたシステムにおけるディジタルコピー制御方法に関し、特にディジタルコピーを制限的に認めつつ、データ作製者の意図しない不許可コピーを効果的に防止するためディジタルコピー制御方法及びそれを用いた装置に関する。

【０００２】

【従来の技術】従来より、ＤＶＤ等の光ディスク再生装置やディジタルＴＶ、ディジタルＶＴＲ等のディジタル記録再生機器をインテリジェントなインタフェースであるＩＥＥＥ１３９４バスを介して相互に接続し、これらディジタル機器間で映像や音楽のコンテンツを送受信するシステムが提案されている。このシステムでは、機器同士でディジタルデータを送受信する際に、それぞれの機器がコンテンツ作成者の意図どおりに動作するものかを確認し、意図どおりに動作しない機器であればデータの転送を禁止することにより、ユーザが映像・音楽コンテンツの作製者の意図しない不許可コピーをしてしまうのを防止することができる。

【０００３】伝送されるディジタルのメインデータの中には、ＣＣＩ（Copy Control Information）と呼ばれるコピー管理情報が含まれている。ＣＣＩは２ビットからなり、“００”が自由にコピー可、“１０”が１回だけコピー可、“１１”がコピー不可を示す。

【０００４】ディジタルデータを送信するとき、送信側機器は、まずＣＣＩによってコンテンツのコピー制限レベルを確認すると共に、ＩＥＥＥ１３９４バス上で受信側機器がコンテンツ作成者の意図どおりに動作するものかどうかを確認する。受信側機器と送信側機器が完全認

証されたら送信側機器からコンテンツが暗号化されて送信される。この場合、送信側機器からのコンテンツのＣＣＩ情報が例えば“１０”の場合でかつ受信側機器が録音機器の場合には、コピー後にＣＣＩを“１１”に書き替えて記録する。これによって、以後のコピーは禁止され、一世代コピーが実現されることになる。

【０００５】一方、ディジタル映像機器の不許可コピーを防止するための別の方法として、ウォーターマークと呼ばれる電子透かし情報を用いる方式も提案されている。この方式は、映像波形などの目立たないところに透かし情報を直接足し込んだり、原信号の周波数変換情報の特定の周波数成分に透かし情報を埋め込むようにしたものである。このウォーターマークにコピー可／不可の情報を与えておくことにより、自由にコピー可、再生のみ可等の指定が可能になる。

【０００６】

【発明が解決しようとする課題】しかしながら、ＣＣＩを用いた従来のコピー制御方法では、受信側機器でＣＣＩを例えば“１０”（１回のみコピー可）から“１１”（コピー不可）に書き替える際に、“１０”を“００”（自由にコピー可）に書き替えることが２ビットの操作で比較的簡単に可能になる。このため、不許可コピーが容易であるという問題がある。

【０００７】また、ウォーターマークを使用する方法は、透かし情報がメインデータ中の映像・音声に係る比較的広い範囲に分散されるため、受信側機器でこれを簡単に書き替えることはできない。ユーザレベルでこれを書き替えようとすると、かなり大規模な回路を備えなければならない。このため、ＣＣＩよりも不許可コピーを防止する点で効果がある。しかしながら、ウォーターマークの書き換えは簡単にできないため、逆にＣＣＩを用いた場合のようにフラグを書き替えてコピーを１回だけ許可するという態様を簡単に採ることができない。

【０００８】この発明は、このような問題点に鑑みなされたもので、コピーを制限する態様を可能にしつつ、許可されないディジタルコピーをより効果的に防止することができるディジタルコピー制御方法及びそれを用いた装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】この発明に係るディジタルコピー制御方法は、バスを介して複数のディジタル機器が接続され、これらディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタル記録媒体からのディジタルデータを送信するに際し、送信側機器および受信側機器は、前記ディジタルデータに含まれるコピー制限のためのコピー管理情報の内容に基づいて不許可コピーを防止するように、当該送信側機器および受信側機器の再生および記録動作の動作制限を行うものにおいて、前記ディジタル記録媒体に記録されるメインデータのうち映像及び／又は音声以外の部分にコピー制限レベルを示す前記コピー管理情報を付加し、また前記メインデータのうち映像及び／又は音声の部分に電子透かし情報を付加すると共に、前記メインデータにエラー訂正コードを追加した後の記録データに特定パターンのエラー情報を意図的に付加し、前記送信側機器で再生されるディジタル記録媒体の正当性を、前記コピー管理情報、電子透かし情報、及び特定パターンのエラー情報の有無により、識別して正当ディスクのデータのみその再生を行い、また適切なデータのみ録音することを特徴とする。

【００１０】この発明に係るディジタル記録媒体の前記メインデータには、映像及び／又は音声以外の部分にコピー制限レベルを示すと共にディジタルコピーを制限する場合ディジタルコピーによって前記コピー制限レベルを強化するように書き替えられるコピー管理情報が含まれ、また、映像及び／又は音声以外の部分にはディジタルコピーによっても書き替えられない電子透かし情報とが外部に読み出し可能な状態で含まれ、前記メインデータ外には、外部に読み出されない媒体マークが付加され、これらコピー管理情報、電子透かし情報、および媒体マークは、これら３種類の情報の内容の組み合わせによって前記メインデータの作成者側の意図するところの、媒体再生管理および媒体コピー管理がなされるように構成されていることを特徴とする。

【００１１】この発明に係るディジタル記録媒体作製装置は、原データにその特徴を損なわない電子透かし情報を付加する透かし情報付加手段と、原データにコピーを制限するためのコピー管理情報を付加するコピー管理情報付加手段と、原データに前記電子透かし情報及びコピー管理情報が付加されたメインデータからエラー訂正コードを生成して付加するエラー訂正コード生成手段と、このエラー訂正コード生成手段でエラー訂正コードが付加されたデータに特定パターンのエラーを媒体マークとして付加するエラー付加手段とを備えたことを特徴とする。

【００１２】また、バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記送信側機器として用いられるこの発明に係るディジタル再生装置は、ディジタル記録媒体から記録データを読み出す読出手段と、この読出手段で読み出された読出データのエラーを検出訂正する誤り検出訂正手段と、この誤り検出訂正手段で検出された誤りが特定パターンになっていることを検出する特定パターン検出手段と、前記誤り訂正手段で誤り訂正されたデータを前記インタフェースの仕様に合ったディジタル情報の形態で前記バスに出力する出力手段と、前記誤り訂正されたデータに含まれるディジタルコピー

を制限するためのコピー管理情報を識別して判定するコピー管理情報判定手段と、前記誤り訂正されたデータからコピー制限レベルを示す電子透かし情報を識別して判定する電子透かし情報判定手段とを備え、前記特定パターンの誤り検出手段の検出結果に基づいて前記ディジタル記録媒体がオリジナル媒体かコピー媒体かを判定し、この判定結果と、前記コピー管理情報判定手段及び前記電子透かし情報判定手段での判定結果により、再生動作の実行又は禁止を行うようにしたことを特徴とする。

【００１３】この発明の１つの具体的態様において、記録媒体中に記録されている情報として、前記コピー管理情報はコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルのいずれかの状態を持ち、前記電子透かし情報はコピーフリー又はコピー禁止の２種類のコピー制限レベルのいずれかを取り、前記追加された特定パターンの誤りに関しては有るか無いかのいずれかの状態を取り、これら各信号の組み合わせで正規に記録されたディスクであるかどうかを判定できるようにして、正規のディスクを識別できるようにしたことを特徴とする。

【００１４】この発明の他の具体的態様においては、前記特定パターン検出手段で特定パターンの誤りが検出され、コピー管理情報判定手段で１世代コピー可と判定され、且つ電子透かし情報判定手段で電子透かし情報がコピー禁止であると判定された場合、再生動作を実行することを特徴とする。

【００１５】この発明の更に他の具体的態様においては、前記特定パターン検出手段で特定パターンの誤りが検出された場合で且つ前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が、コピー管理情報が１世代コピー可で且つ電子透かし情報がコピー禁止となっている場合を除いて相矛盾する内容となっているとき、又は前記特定パターン誤り検出手段で特定パターンの誤りが検出された場合で且つ前記電子透かし情報が検出出来なかった場合、再生を行わないことを特徴とする。

【００１６】この発明の更に他の具体的態様においては、前記特定パターン誤り検出手段で特定パターンの誤りが検出されなかった場合で且つ、前記コピー管理情報判定手段と前記電子透かし情報判定手段の判定結果が異なる場合、再生を行わないことを特徴とする。

【００１７】更に、この発明に係るディジタル記録装置は、バスを介して接続された複数のディジタル機器間で相互に認証処理を行い、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介して、送信側機器から受信側機器にディジタルデータを送信するシステムの前記受信側機器として用いられるディジタル記録装置において、映像及び／又は音声以外の部分にコピーフリー、１世代コピー可又はコピー禁止の３種類のコピー制限レベルを示す前記コピー管理情報が付加されると共に、映像及び／又は音声の部分にコピー可又はコピー禁止の２種類の電子透かし情報が付加されたディジタルデータを受信する受信し、識別されたコピー管理情報が１世代コピー可で、且つ識別された電子透かし情報がコピー禁止である場合、電子透かし情報はそのまま記録し、コピー管理情報のみコピー禁止に書き換えて記録することを特徴とする。

【００１８】この発明によれば、３種類の情報によってディジタル記録媒体の正当性を判定する。第１の情報は、メインデータのうち映像・音声以外の部分に含まれるコピー制限レベルを示すコピー管理情報で、ディジタルコピーを制限する場合、コピーされるとコピー制限レベルが強化されるように書き替えられる。第２の情報は、同じくメインデータのうち映像・音声の部分に含まれてコピー制限レベルを示す電子透かし情報で、この情報はディジタルコピーされても書き替えられないし、書き換えは極めて困難である。第３の情報は、エラー訂正後のデータに意図的に付加される特定パターンのエラー情報（以下、媒体マークと呼ぶ）で、この情報は、メインデータ外に付加されるものであるから、記録媒体から再生されたメインデータには含まれず、ディジタルコピーされると消失する。

【００１９】このように、３つの情報がそれぞれ異なる性質を持っているので、これら３つの情報の状態によってディジタル記録媒体が正当にコピーされたものかどうかを詳細に判定することができる。即ち、まず、媒体マークは、１回ディジタルコピーされると消失するので、媒体マークの有無によって、それがオリジナル媒体かコピー媒体かが判定できる。また、コピー管理情報と電子透かし情報とは、共にコピー制限レベルを示すものであるが、自由にディジタルコピー可の媒体の場合、コピー管理情報と電子透かし情報とは、いずれも自由にコピー可を示す組合せのみ有効であり、その他はコピー管理情報が正規の処理を経ずに書き替えられた可能性があるので、媒体マークの検出されない媒体は正当でない媒体と認識することができる。また、ある制限の下にコピーを許容する場合には、コピー管理情報と電子透かし情報とが共にコピー制限レベルを示すものでなければならず、いずれか一方が自由にコピー可を示す場合には、これも正当でない媒体である。更に、コピー管理情報と電子透かし情報とがいずれも所定のコピー制限レベルを示す場合には、コピーによってコピー管理情報のみが書き替えられるが、このとき、コピー管理情報がコピー制限レベルを低下又は現状維持するように意図的に書き替えられても、媒体マークの消失によってこれが認識され、正当でない媒体であると判定することができる。

【００２０】送信側機器で、このような判定の結果、正当でない媒体であると認定された場合には、送信側機器がディジタルデータの再生を禁止するので、その媒体は、再生も記録もできず、これにより不許可コピーを効

果的に防止することができる。また、送信側機器が正当な媒体であると認識した場合には、そのコピー制限レベルに応じて記録再生可又は再生のみ可となるように、認証した受信側機器にディジタルデータを送信するので、制限された条件下でのディジタルコピーも可能になる。

【００２１】また、認証された機器間では、アナログ信号経由でディジタル記録することが可能な場合にも、これら認証された機器間でのみ認証し合あえる電子認証署名データをディジタルデータコンテンツと共に記録するようにし、上述した認識手法に加え、さらにこの認証が成立した場合にのみ、データコンテンツの再生を許可するようにすれば、データコンテンツそのものの不許可コピーをより確実に防止できる。

【００２２】

【発明の実施の形態】以下、図面を参照して、この発明の好ましい実施の形態について説明する。図１は、この発明の一実施例に係るディジタルデータ送受信システムの構成を示すブロック図である。送信側機器であるＤＶＤプレーヤ１と、受信側機器であるディスプレイ装置２及びＤＶＤレコーダ３は、ＩＥＥＥ１３９４仕様に準拠したそれぞれのインタフェース４，５，６及びバス７を介して相互に接続されている。ＤＶＤプレーヤ１は、送信ソースとなる映像・音楽コンテンツが記録されたＤＶＤ８を再生して得られたディジタルデータを、バス７を介してディスプレイ２及びレコーダ３に伝送する。レコーダ３は、ディジタルコピーが許可されているディジタルデータである場合に限り、受信したディジタルデータをＤＶＤ９に記録する。

【００２３】プレーヤ１は、ＤＶＤ８の再生に先立ち、ディスプレイ装置２及びレコーダ３との間でこれら各機器がコンテンツ作成者の意図どおりに動作する機器であるかどうか相互認証処理を実行する。例えば、例えばディスプレイ装置２には、記録機能が無いので、プレーヤ１との間には公開鍵を用いた完全認証が成立する。この場合、記録が禁止されているコンテンツでも再生が可であればデータが転送される。プレーヤ１とレコーダ３との間は、共通鍵を用いた制限付き認証が成立する。この場合、記録も再生も可であるコンテンツのみがデータ転送される。認証された機器間でのみデータ転送が有効となるように、バス７上のデータは暗号化される。

【００２４】また、プレーヤ１は、再生しようとするＤＶＤ８が正当な媒体であるかどうかを、ＤＶＤ８に記録されている３種類の情報、即ち、ＣＣＩ（コピー管理情報）、ウォーターマーク（電子透かし情報）及びメディアマーク（媒体マーク：特定パターンのエラー情報）によって検証する。

【００２５】図２は、これら情報が付加されたＤＶＤの原盤を作製する原盤作製装置の構成を示すブロック図である。記録すべき原信号は、ウォーターマーク付加部１１で、原信号の目立たない部分、例えばマスキング効果がある輝度差の大きな部分等に、ウォーターマークを埋め込む。また、ウォーターマークは、原信号をフーリエ変換した信号の特定の周波数に埋め込むようにしてもよい。ウォーターマークが埋め込まれた信号はエンコーダ１２によって圧縮符号化されるが、ここまでの過程のいずれかで、内部の図示しないＣＣＩ付加手段によって、作製者の意図する２ビットのＣＣＩが付加されている。ここではエンコーダ１２でＣＣＩを付加している。次にＩＤ／ＥＤＣ付加部１３でＩＤやエラー検出コードが付加された後、ＥＣＣ生成部１４でエラー訂正コードが付加される。エラー訂正コードが付加されたデータは、例えば１％程度の読み取りエラーに耐えられるものである。ここでは、そのようなエラーレートを超えない程度に、エラー付加手段１５によって特定パターンのエラー情報をメディアマークとして付加する。つまり意図的にビット誤りを生じさせる。メディアマークは、時間軸上のパターンでも周波数軸上でのパターンでもよい。メディアマークが付加されたデータは、ＥＦＭ変調部１６で、８→１６（ＤＶＤ）又は８→１４（ＣＤ）変調され、記録ドライバ１７によって原盤ディスク１８に記録される。この原盤１８によって作製されたＤＶＤがオリジナル版となる。

【００２６】図３は、図１のプレーヤ１の詳細を示すブロック図である。ＤＶＤ８に記録された記録データは、読出ヘッド２１によって読み出され、ＥＦＭ復調部２２で復調されたのち、ＥＣＣ復調部２３でエラー訂正処理がなされる。メディアマーク検出部２４は、ＥＣＣ復調部２３でのエラーパターンの傾向を相関演算等によって求め、予め決められた特定のパターンでエラーが発生している場合には、メディアマーク有りと判定する。メディアマーク検出部２４からの出力は出力制御部２６に供給される。ＥＣＣ復調部２３で復調されたデータは、ＣＣＩ判定部２８、ウォーターマーク判定部２７を経てデコーダ２５に供給される。ウォーターマーク判定部２７及びＣＣＩ判定部２８は、それぞれ抽出されたウォーターマーク及びＣＣＩを判定し、出力制御部２６に判定結果を出力する。なお、ウォーターマーク等の記録方式によっては、信号復号処理中ではなく、その前或いは後で判定するようにしても良い。出力制御部２６は、メディアマーク検出部２４の検出出力とウォーターマーク判定部２７及びＣＣＩ判定部２８の判定結果とから、データ伝送が可能と判断した場合、デコーダ２５からウォーターマーク及びＣＣＩを含む伝送すべきメインデータをＩ／Ｆ２９に供給するように制御する。また、プレーヤの再生を禁止する場合には、必要に応じて再生制御部３１を制御する。そしてＩ／Ｆ２９にデータが供給された場合には、伝送すべきメインデータはＩＥＥＥ１３９４に準拠する固定ビットレートに変換されてバス７上に出力される。

【００２７】一方、レコーダ３は、メインデータが伝送

されてきた場合には、コピー可の状態であるからこれをディジタルコピーするが、メインデータに含まれるウォーターマーク及びＣＣＩがある制限下でのみコピー可を示している場合には、コピーと同時にＣＣＩを制限レベルが上がるように書き替える。

【００２８】図４は、出力制御部２６が判断するメディアマーク、ウォーターマーク及びＣＣＩと再生及び記録の可／不可を示す表である。メディアマークは、上述したように、伝送すべきメインデータには含まれていないので、コピーディスクには存在しない。また、ＤＶＤやＣＤの旧ディスクにも当然含まれていない。このため、メディアマークが存在するディスクはオリジナルディスク、存在しないディスクはコピーディスク又は旧ディスクと判断することができる。

【００２９】ウォーターマークは、自由にコピーを許容する場合には“００”、コピーを制限する場合には“１１”に設定される。ＣＣＩは、“００”で自由にコピー可、“１０”で１回だけコピー可、“１１”でコピー不可とする。ウォーターマークが存在しない場合には、旧ディスクであるから、ウォーターマーク無しでメディアマーク有りという組合せは矛盾する。従って、この場合にはＣＣＩのパターンに拘わらず無効（正当でない）とする。また、メディアマーク、ウォーターマークが共に無い場合には、旧ディスクであるから、ＣＣＩに応じて自由にコピー可（００）、１回だけコピー可（１０）、再生のみ可（１１）とする。

【００３０】ウォーターマークとＣＣＩが共に“００”の場合には、自由にコピー可であるから、メディアマークの有無に拘わらず記録・再生を許可する。しかし、ウォーターマークが“００”で、ＣＣＩが“１０”又は“１１”の場合には、矛盾が生じるので、意図的なビット操作がなされたと考えて正当でないディスクとする。

【００３１】ウォーターマークが“１１”のときは制限付きコピーであるから、ＣＣＩは、“１０”又は“１１”となる。従って、ＣＣＩが“００”のときは、正当でないディスクと取り扱う。ＣＣＩが１回だけコピー可（１０）のときは、オリジナルディスクでなければならないので、メディアマークがある時のみ有効で、無いときにはＣＣＩを意図的に書き換えした正当でないディスクと判定する。ＣＣＩが“１１”のときには、コピー禁止であるから、再生のみ可とする。

【００３２】以上の判断により、ＤＶＤ８が正当でないディスクであると判定された場合には、再生も記録も許可しないので、プレーヤ１は、ディスプレイ装置２にもレコーダ３にもメインデータを伝送しない。また、再生のみ可と判断された場合には、ディスプレイ装置２、レコーダ３へメインデータを伝送するが、認証を受け得る構成であるレコーダ３は、そのデータが再生のみとのＣＣＩを有しているので、記録動作は行わない。

【００３３】なお、この再生及び記録の可否制御の考え方は、実施例に示したディジタルデータ伝送システムに限らず、従来から存在したアナログ信号を使った伝送によるディジタル再生・記録機器のシステムにも良く合致する。例えば、図４に示すように、入力ソースとしてアナログ入力が用いられた場合、ウォーターマークは入れられるので、その場合には、メディアマーク無し、且つＣＣＩはウォーターマークに準ずると見なせば、この発明と同様に処理できる。また、ディジタル放送波を入力する場合には、登録されたディジタル放送波を受信できていることをもってメディアマーク有りと見れば、後のウォーターマーク、ＣＣＩも全く問題なく付与できるので、この発明と同様に処理できる。

【００３４】また、先に説明したような、複数のディジタル機器がバスを介して接続され、これらディジタル機器間で相互に認証処理が行われ、認証された機器間でのみディジタルデータの送受信が行われるインタフェースを介するディジタルデータ伝送システムであったとしても、正当な媒体に記録されたものであればその音声及び／又は映像の再生内容をアナログ信号として出力でき、この出力について、認証された機器以外の非認証の機器または違法な機器を用い、再度別の記録媒体にディジタル記録されてしまう可能性が残る。このような記録媒体は、認証機器システムでは、ウォーターマーク、またはメディアマークを持たない旧システムの媒体として認識せざるを得ず、さらにはそのＣＣＩがコピーフリーまたは１世代コピー可と記録されていると、この媒体が今一度認証機器システム間に持ち込まれた場合、再生は勿論のこと、１世代コピー可のＣＣＩに基づいて、認証機器システム自体で再度コピー媒体を作成してしまうことになり、正当でない媒体から正当な媒体が作られてしまう可能性がある。アナログ出力を一切禁止することは勿論実施できるはずはなく、また、アナログ出力にエンクリプション（暗号化）を施すということも、再生側機器全てに、例えば世の中にある全ての映像ディスプレイ装置に暗号解読回路を組み込むことも実際上実現不可能である。

【００３５】このような非認証機器を用いて作成された正当でない媒体を、認証された機器で再生できないようにするには、認証された機器における記録及び／又は再生動作に、これら認証機器システム間でのみ認識できる電子認証署名データを追加利用するように構成すれば良い。これにより認証機器システム間ではこの電子認証署名により、その媒体の記録データが認証機器システム内で正当に記録されたものか否かが確認でき、そのうえで再生及び／又は記録動作の実行を制御することが可能となる。したがって、非認証の機器を用いて記録された、正当でない媒体データを認証機器システム内のいずれかの機器で再生しようとしても、認証機器システム間で行われるべき電子認証署名が存在しないか、または電子認証署名の認証結果が不成立となり、この場合には再生動

作を行わない様にする事によって、正当でない媒体の使用を防止できる。

【００３６】電子認証署名の生成・認証については、種々のデータ暗号化方式を利用できるが、ここでは例えば公開鍵暗号化方式を応用したものを利用した例を説明する。公開鍵暗号化方式として代表的なＲＳＡ（Rivest,Shamir,Adleman)暗号は大きな数の素因数分解の困難さに安全性の根拠をおき、べき乗剰余の計算により暗号化／復号化処理を行うものである。暗号化手順は「Ｃ＝Ｅ（Ｍ）＝（Ｍのｅ乗）剰余ｎ）」で表され、復号化手順は「Ｍ＝Ｄ（Ｃ）＝（Ｃのｄ乗）剰余 ｎ」で表される。ここで、Ｍは平文、Ｃは暗号文である。暗号化鍵はｅとｎ、復号化鍵はｄとｎで、暗号化鍵ｅと共通鍵ｎは公開し、復号化鍵ｄは秘密とする。鍵ｅ，ｄ，ｎの決定は次の手順で行う。（１）２つの大きな素数ｐ，ｑを任意に選び、ｎ＝ｐｑとする。（２）（ｐ－１）と（ｑ－１）の最小公倍数Ｌを計算し、Ｌと互いに素でＬより小さな任意の整数ｅを求める。（３）ｅｄ＝１剰余Ｌを満たすｄを求める。こうして選んだ値ｅ，ｄ，ｎは、全ての平文Ｍに対し、「（Ｍのｅｄ乗）剰余ｎ＝Ｍ」が成立する。解読者が暗号文Ｃを解読するには復号化鍵ｄを知らなければならないが、そのためには秘密の素数ｐ，ｑを知り、（ｐ－１）および（ｑ－１）の最小公倍数Ｌと公開鍵ｅとから「ｄ＝ｅの－１乗剰余Ｌ」を演算し、秘密鍵ｄを求める必要がある。公開鍵ｎは素数ｐおよびｑの積であるから公開鍵ｎが容易に素因数分解できる程度の整数では暗号にならない。そこで通常はｐとｑを各１００桁（十進数）程度とし、公開鍵ｎは２００桁程度としている。こうすれば、１０００ＭＩＰＳの電子計算機を用いても素因数分解に数百万年かかる勘定になり、実質的に解読は不可能である。

【００３７】具体的な認証機器システム内の機器の動作を説明する。まず認証機器システム内の各機器には予め共通鍵ｎが記憶されている。これら機器は記録すべきデータコンテンツを媒体に書き込む際に機器内で、自己の機器認識ＩＤおよび記録すべきコンテンツの固有ＩＤを組み合わせた内容を公開されている暗号化鍵ｅで暗号化して電子認証署名のデータとして作成し、これを記録すべきデータコンテンツと共に媒体に記録する。この媒体を認証機器システム内のいずれかの機器で動作させる場合には、共通鍵と外部非公開の秘密復号化鍵を用いて復号化し、機器ＩＤとデータコンテンツＩＤを確かめ、正当と認められる場合のみ、これを再生するように制御する。もしもこのデータ媒体が、非認証の機器により記録されたものであると、電子認証署名のデータがないか、あるいは、復号化不能のもの（認証機器システム間で共通する特定の暗号化がなされていないの）となり、もってこれを正当な媒体と認めることはなく、また、そのようなデータコンテンツは、再生されることはない。

【００３８】

【発明の効果】以上述べたように、この発明によれば、３種類の異なる性質の情報を組み合わせることにより、ディジタル記録媒体が正当なものかどうかを明確に判定することができ、これによりコピーを制限する態様を可能にしつつ、正当でないディジタルコピーをより効果的に防止することができるという効果を奏する。

【図面の簡単な説明】

【図１】　この発明の一実施例に係るディジタルデータ伝送システムのブロック図である。

【図２】　この発明を適用したディスクの原盤作製装置のブロック図である。

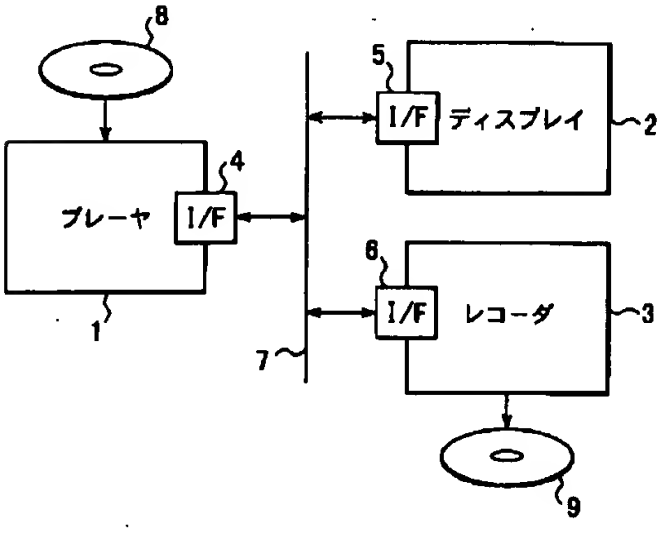
【図３】　図１のシステムのプレーヤの詳細ブロック図である。

【図４】　この発明で使用される３種類の情報と記録及び再生の可／不可の対応関係を示す図である。

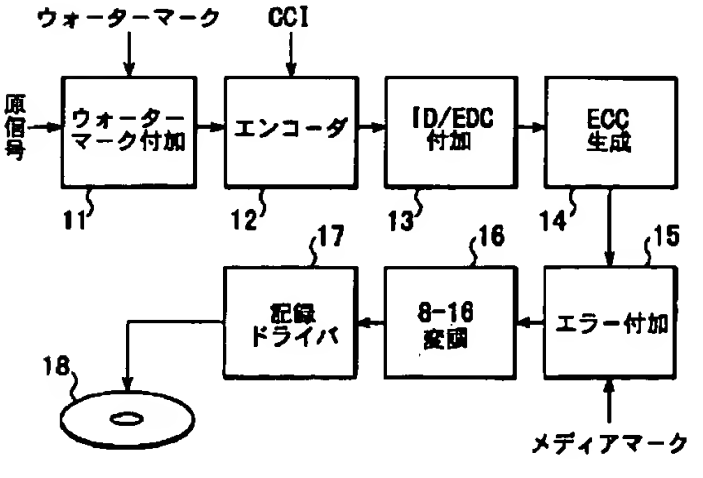
【符号の説明】

１…プレーヤ、２…ディスプレイ装置、３…レコーダ、４，５，６…インタフェース、７…バス。

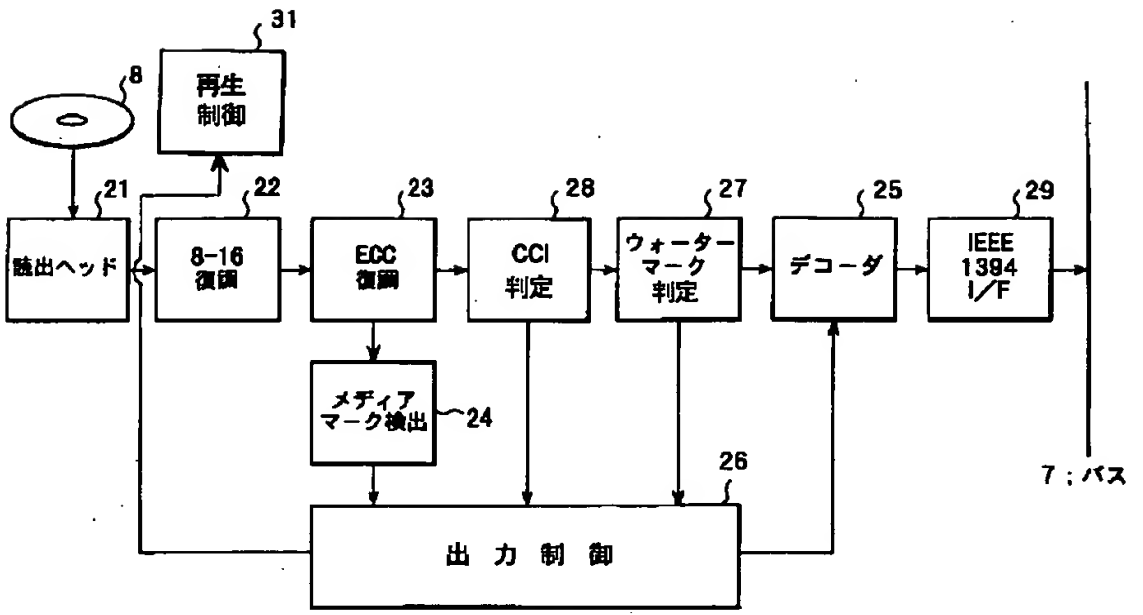
【図１】



【図２】



【図３】


31
再生
制御
8
21
22
23
28
27
25
29
読出ヘッド
8-16
復調
ECC
復調
CCI
判定
ウォーター
マーク
判定
デコーダ
IEEE
1394
I/F
メディア
マーク検出
24
26
出力制御
7：バス

【図4】

入力の状態	入力コンテンツのフラグ		入力ソースの素性			再生コントロール	再生出力時のフラグ		録音コントロール	録音後		説明
	Water Mark	CCI	システム	正当性	概要		Water Mark	CCI		Water Mark	CCI	
メディアマーク有りディスク	11	11	新	正規	録音禁止	○	11	11	×	−	−	正規の録音禁止ディスク
	11	10	新	正規	一世代コピー可	○	11	10	○	11	11	正規の一世代コピー可のオリジナルディスク
	11	00	新	不正	不正改造	×			×	−	−	不正改造ディスク、新装置では再生不可能
	00	11	新	不正	不正改造	×			−	−	−	正規の組み合わせには無い
	00	10	新	不正	不正改造	×			−	−	−	正規の組み合わせには無い
	00	00	新	正規	コピーフリー	○	00	00	○	00	00	オリジナルのコピーフリーディスク
	無し	11	新	不正	不正改造	×			−	−	−	意味の無い組み合わせ（改造）
	無し	10	新	不正	不正改造	×			−	−	−	意味の無い組み合わせ（改造）
	無し	00	新	不正	不正改造	×			−	−	−	意味の無い組み合わせ（改造）
メディアマーク無しディスク := デジタル入力	11	11	新	正規	一世代コピー可ディスクのコピー	○	11	11	−	−	−	一世代コピー可のコンテンツの録音ディスク：不正コピーディスクの可能性有り
	11	10	新	不正	不正改造	×			×	−	−	不正コピーディスク
	11	00	新	不正	不正改造	×			×	−	−	不正コピーディスク
	00	11	新	不正	不正改造	×			×	−	−	意味の無い組み合わせ（改造）
	00	10	新	不正	不正改造	×			×	−	−	意味の無い組み合わせ（改造）
	00	00	新	正規	コピーフリーディスクのコピー	○	00	00	○	00	00	コピーフリーディスクのコピーディスク
	無し	11	旧	正規	コピー禁止	○	無し	11	×	無し	11	旧ディスクの為、不正防止は弱い（CCIのみ）
	無し	10	旧	正規	一世代コピー可	○	無し	10	○	無し	11	旧ディスクの為、不正防止は弱い
	無し	00	旧又は個人製作ディスク	正規	コピーフリー	○	無し	00	○	無し	00	旧ディスクの為、不正防止は弱い
アナログ入力	11	−	新	正規	コピー禁止	○	11	11*	×	−	−	アナログでもコピーコントロールが可能
	00	−	新	正規	コピーフリー	○	00	00*	○	00	00	アナログでもコピーコントロールが可能
	無し	−	旧ディスク又は個人製作ディスク	正規＋旧不正	1世代コピー可	○	無し	10*	○	無し	11	1世代のみコピー可とする。（SCMSと同等）
放送波	11	11	新システム	正規	コピー禁止	○	11	11	×	−	−	基本的に不正信号は出てこない
	11	10	新システム	正規	一世代コピー可	○	11	10	○	11	11	基本的に不正信号は出てこない
	00	00	新システム	正規	コピーフリー	○	00	00	○	00	00	基本的に不正信号は出てこない
	無し	11	現状システム	正規	コピー禁止	○	無し	11	×	−	−	基本的に不正信号は出てこない
	無し	10	現状システム	正規	一世代コピー可	○	無し	10	○	無し	11	基本的に不正信号は出てこない
	無し	00	現状システム	正規	コピーフリー	○	無し	00	○	無し	00	基本的に不正信号は出てこない

11*，00*，10*は、それぞれ11，00，10として扱うという意味

<HTML><HEAD><META HTTP-EQUIV="Content-Type"
CONTENT="text/html;charset=Shift_JIS"><TITLE>JP-A-2000-48478</TITLE></HEAD><BODY>
<CENTER><H2><B>PATENT ABSTRACTS OF JAPAN</B></H2></CENTER><TABLE BORDER="0"
WIDTH="100%"><TR><TD WIDTH="40%" VALIGN="top">
</TD><TD WIDTH="15%"
NOWRAP>(11)Publication number : </TD><TD VALIGN="top"
WIDTH="45%"><B>2000-048478</B></TD></TR><TR><TD WIDTH="40%"
VALIGN="top">
</TD><TD WIDTH="15%" NOWRAP>(43)Date of publication of application
: </TD><TD VALIGN="top" WIDTH="45%"><B>18.02.2000</B></TD></TR></TABLE><HR
WIDTH="100%" SIZE="5"><TABLE BORDER="0" WIDTH="100%"><TR><TD VALIGN="top"
WIDTH="40%">(51)Int.Cl.</TD><TD VALIGN="top" WIDTH="60%"><PRE><B>   G11B
20/10</B>
</PRE></TD></TR></TABLE><HR WIDTH="100%" SIZE="5"><TABLE BORDER="0"
WIDTH="100%"><TR><TD WIDTH="15%" NOWRAP VALIGN="top">(21)Application number :
</TD><TD WIDTH="25%" VALIGN="top"><B>10-192084</B></TD><TD WIDTH="15%" NOWRAP
VALIGN="top">(71)Applicant : </TD><TD WIDTH="45%" VALIGN="top"><B>YAMAHA
CORP
</B></TD></TR><TR><TD WIDTH="15%" NOWRAP VALIGN="top">(22)Date of filing :
</TD><TD WIDTH="25%" VALIGN="top"><B>07.07.1998</B></TD><TD WIDTH="15%" NOWRAP
VALIGN="top">(72)Inventor : </TD><TD WIDTH="45%" VALIGN="top"><B>MATSUMOTO
SEIJI
FURUKAWA MASAMICHI
</B></TD></TR></TABLE><HR WIDTH="100%"
SIZE="5"><TABLE BORDER="0"><TR><TD>(30)Priority</TD></TR><TR><TD
VALIGN="top">Priority number : </TD><TD VALIGN="top" NOWRAP><B>10161361

</B></TD><TD VALIGN="top">   Priority date : </TD><TD
VALIGN="top"><B>26.05.1998
</B></TD><TD
VALIGN="top">   Priority country : </TD><TD
VALIGN="top"><B><NOBR>JP
</NOBR></B></TD></TR></TABLE><HR WIDTH="100%"
SIZE="5"><TABLE BORDER="0" WIDTH="100%"><TR><TD>(54)<B> DIGITAL COPY CONTROL
METHODAND DEVICE USING THE METHOD
</B></TD></TR><TR><TD
VALIGN="top">(57)Abstract:
PROBLEM TO BE SOLVED: To clearly decide whether or not
a digital recording medium is a authorized one by discriminating it with the
presence of copy control informationelectronic watermark information and error
information of a specified patternreproducing only the data of authorized disks and
recording only the proper data.
SOLUTION: A player 1 executes mutual
certification processing of whether or not respective equipments are operated as an
intention of a contents former between a display device 2 and a recorder 3 prior to
reproduce a DVD. The certification with a limit using a common key is formed between
the player 1 and the recorder 3and only the recordable and reproducible contents are
data transferred. The data on a bus 7 are ciphered so that the data transfer is
validated only between the certified equipments. Furtherthe player 1 verifies
whether or nor the DVD 8 to be reproduced is a legal medium by three kinds of
information recorded on the DVD 8that isthe copy control informationthe electronic
watermark information and the error information of the specified
pattern.

</TD></TR></TABLE><!-- 20071127 delete<HR WIDTH="100%"
SIZE="5">LEGAL STATUS<TABLE BORDER="0" WIDTH="100%"><TR><TD WIDTH="50%">[Date of
request for examination]</TD><TD WIDTH="50%" VALIGN="top"
ALIGN="left"></TD></TR><TR><TD WIDTH="50%" VALIGN="top">[Date of sending the
examiner's decision of rejection]</TD><TD WIDTH="50%" VALIGN="top"
ALIGN="left"></TD></TR><TR><TD WIDTH="50%" VALIGN="top">[Kind of final disposal of
application other than the examiner's decision of rejection or application converted
registration]</TD><TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD></TR><TR><TD
WIDTH="50%" VALIGN="top">[Date of final disposal for application]</TD><TD
WIDTH="50%" VALIGN="top" ALIGN="left"></TD></TR><TR><TD WIDTH="50%"
VALIGN="top">[Patent number]</TD><TD WIDTH="50%" VALIGN="top"
ALIGN="left"></TD></TR><TR><TD WIDTH="50%" VALIGN="top">[Date of
registration]</TD><TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD></TR><TR><TD
WIDTH="50%" VALIGN="top">[Number of appeal against examiner's decision of
rejection]</TD><TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD></TR><TR><TD
WIDTH="50%" VALIGN="top">[Date of requesting appeal against examiner's decision of
rejection]</TD><TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD></TR><TR><TD
WIDTH="50%" VALIGN="top">[Date of extinction of right]</TD><TD WIDTH="50%"
VALIGN="top" ALIGN="left"></TD></TR></TABLE>20071127 delete
--><!--__CORRECT_DELETE__<HR WIDTH="100%" SIZE="5">CORRECTION
<TABLE
BORDER="0">__CORRECT_DATA__</TABLE>__CORRECT_DELETE__--><HR><B>CLAIMS</B>
<HR><SD
O CLJ><DP N=0002><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>[Claim(s)]
[Claim
1]Via an interface which two or more digital equipment is connected via a busand

performs authenticating processing mutually among these digital equipment and with which transmission and reception of digital data are performed only between attested apparatusFrom transmitting side apparatusface transmitting digital data from a digital recording medium to receiver apparatusand transmitting side apparatus and receiver apparatusSo that a disapproval copy may be prevented based on the contents of copy management information for copy restrictions included in said digital dataIn a digital copy control method of performing reproduction of the transmitting side apparatus concerned and receiver apparatusand restriction of recording operation of operationSaid copy management information which shows a copy restriction level is added to portions other than an image and/or a sound among main data recorded on said digital recording mediumAdd electronic watermark information to portions of an image and/or a sound among said main dataand. Add error information of a specific pattern to record data after adding an error correction code to said main data intentionallyand the justification of a digital recording medium reproduced by said transmitting side apparatus is identified by existence of said copy management informationelectronic watermark informationand error information of a specific patternA digital copy control methodwherein only data of a just digital recording medium performs the reproduction and only suitable data records it.
[Claim 2]Reproduction or in order to record separatelymain data in a digital recording medium which it comes to record to said main data. Copy management information rewritten so that said copy restriction level may be strengthened by a digital copywhen restricting a digital copywhile a copy restriction level is shown in portions other than an image and/or a sound is includedIn the state in which read-out outside is possibleit is included in portions other than an image and/or a sound by electronic watermark information which is not rewritten by digital copyeitherand besides said main dataIt is added by medium mark which is not read outside and these copy management informationelectronic watermark informationand a medium markA digital recording medium constituting so that medium reproduction management and medium copy management by the side of a maker of said main data to mean may be made with combination of the contents of these three kinds of information.
[Claim 3]A <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>digital recording medium manufacturing device comprising:
A watermark information addition means which adds electronic watermark information which does not spoil the feature to original data.
A copy-management-information addition means which adds copy management information for restricting a copy to original data.
An error correction code creating means which generates and adds an error correction code from main data in which said electronic watermark information and copy management information were added to original data.
An error addition means which adds an error of a specific pattern to data in which an error correction code was added by this error correction code creating means as a medium mark.

[Claim 4]Have the followingand said digital recording medium judges an original medium or a copy medium based on a detection result of said specific pattern error detection meansand it This decision result. It is characterized by being based on a decision result in said copy-management-information judging means and said electronic-watermark-information judging meansand permitting or forbidding reproduction of data of said transmitting side apparatus. Via an interface which performs authenticating processing mutually among two or more digital equipment connected via a bus and with which transmission and reception of digital data are performed only between attested apparatusDigital playback equipment used as said transmitting side apparatus of a system which transmits digital data to receiver apparatus from transmitting side apparatus.
A reading means which reads record data from a digital recording medium.
An error detection correcting means which extracts an error correction code from read-out data read by this reading meansand carries out detection correction of the error of read-out data based on this error correction code.
A specific pattern error detection means to detect that an error detected by this error detection correcting means is a specific pattern.
An output means which outputs data by which the error correction was carried out by said error detection correcting means to said bus with a gestalt of digital information suitable for specification of said interfaceA copy-management-information judging means which identifies and judges copy management information for restricting a digital copy contained in said data by which the error correction was carried outand an electronic-watermark-information judging means which identifies and judges electronic watermark information which

shows a copy restriction level from said data by which the error correction was carried out.

[Claim 5]Discriminate said copy-management-information judging means from said copy management informationand a copy freelancerand that an one-generation copy is possible or three kinds of copy restriction levels of copy prohibition said electronic-watermark-information judging meansDiscriminate a copy freelancer or two kinds of copy restriction levels of copy prohibition from said electronic watermark informationand said specific pattern error detection meansThe digital playback equipment according to claim 4 identifying existence of an error of said specific patternjudging whether it is the disk regularly recorded from a discriminated result in these each meansand playing only a regular disk.
[Claim 6]An error of a specific pattern is detected by said specific pattern error detection meansand it is judged with an one-generation copy being possible by a copy-management-information judging meansAnd the digital playback equipment according to claim 5 characterized by performing reproduction motion when judged with electronic watermark information being copy prohibition by an electronic-watermark-information judging means.
[Claim 7]By a case where an error of a specific pattern is detected by said specific pattern error detection meansand a <DP N=0003><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>decision result of said copy-management-information judging means and said electronic-watermark-information judging meansWhen it is contents which conflict except for a case where an one-generation copy of copy management information is possibleand electronic watermark information serves as copy prohibitionOr the digital playback equipment according to claim 4 or 5 characterized by not reproducing when an error of a specific pattern is detected by an error detection means of said specific patternand when said electronic watermark information is not able to be detected.
[Claim 8]The digital playback equipment according to claim 4 or 5 characterized by not reproducing when an error of a specific pattern is not detected by an error detection means of said specific patternand when decision results of said copy-management-information judging means and said electronic-watermark-information judging means differ.
[Claim 9]Via an interface which performs authenticating processing mutually among two or more digital equipment connected via a bus and with which transmission and reception of digital data are performed only between attested apparatusIn a digital recording device used as said receiver apparatus of a system which transmits digital data to receiver apparatus from transmitting side apparatusA copy freelancer and said copy management information which an one-generation copy is possible or shows three kinds of copy restriction levels of copy prohibition are added to portions other than an image and/or a soundand. An one-generation copy of copy management information which receives digital data in which a copy was possible into portions of an image and/or a soundor two kinds of electronic watermark information of copy prohibition were added to them and which was received and identified is possibleAnd a digital recording device when identified electronic watermark information is copy prohibitionwherein it records electronic watermark information as it is and it rewrites and records only copy management information on copy prohibition.
[Claim 10]Apparatus constituted via said interface by said attested apparatus in digital data contents recorded on a digital recording medium so that an output was possible as an analog signalAnd apparatus constituted via said interface in data contents inputted with an analog signal so that record to a new digital recording medium was possible is includedWhen all the these-attested apparatus carries out digital recording of the data contents supplied with an analog signal or a digital signal to a digital recording mediumAre constituted so that electronic authentication signature data which can be attested only between the attested apparatus concerned may be recorded on the medium concerned in addition to data contentsand. When reproducing digital data contents recorded on a digital recording mediumA digital copy control method according to claim 1 controlling to reproduce digital data contents of the medium concerned only when it is detected and attested whether electronic authentication signature data which can be attested only between said attested apparatus exists on the medium concerned.
[Claim 11]The <TXF FR=0002 HE=085 WI=080 LX=1100 LY=0300>digital recording medium according to claim 2 characterized by coming to record electronic authentication signature data which can be attested only between attested apparatus further.
[Claim 12]The digital playback equipment according to claim 4 having further a means to forbid reproduction of data when electronic authentication signature data is not attested with a means to detect electronic authentication signature data which can be

attested only between attested apparatus.
[Claim 13]In digital data contents recorded on a digital recording mediumvia said interfacesaid at least some of attested apparatus is constituted so that an output is possible as an analog signalWhen carrying out digital recording of the data contents supplied with these analog signals to a digital recording mediumThe digital recording device according to claim 9 constituting so that electronic authentication signature data which can be attested only between the attested apparatus concerned may be recorded on the medium concerned in addition to data contents.
</SDO>
<HR><B>DETAILED DESCRIPTION</B>
<HR><SDO DEJ><TXF FR=0003 HE=165 WI=080 LX=1100 LY=1150>[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention A DVD (digital video disc) recording and reproducing deviceAccepting especially a digital copy restrictively about the digital copy control method in the system to which digital equipmentsuch as a digital video tape recorder and digital TVwas connected via the interface provided with the mutual recognition function. In order to prevent effectively the disapproval copy which data production persons do not meanit is related with the digital copy control method and the device using it.
[0002]
[Description of the Prior Art]From beforedigital recording playback apparatussuch as optical disk reproducing devices and digital TVssuch as DVDand a digital video tape recorderis mutually connected via the IEEE1394 bus which is an intelligent interfaceThe system which transmits and receives the contents of an image or music among these digital equipment is proposed. By forbidding a data transfer in this systemif each apparatus is apparatus which checks whether it is what operates as a contents creator's intentionand does not operate as an intention when transmitting and receiving digital data by apparatusA user can prevent carrying out the disapproval copy which the production persons of an image and a music content do not mean.
[0003]In the digital main data transmittedthe copy management information called CCI (Copy Control Information) is included. CCI consists of 2 bitsfreely00shows a copy good10shows a copy goodand "11" shows a copy failure only once.
[0004]When transmitting digital datathe copy restriction level of contents is first checked by CCIand transmitting side apparatus checks whether it is that to which receiver apparatus operates as a contents creator's intention on an IEEE1394 bus. <DP N=0004><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>If full attestation of receiver apparatus and the transmitting side apparatus is carried outcontents will be enciphered and transmitted from transmitting side apparatus. In this casewhen the CCI information on the contents from transmitting side apparatus is "10"and when receiver apparatus is a recorder machineCCI is rewritten and recorded on "11" after a copy. Future copies will be forbidden by this and a time cost copy will be realized.
[0005]On the other handthe method using the electronic watermark information called a watermark is also proposed as an option for preventing the disapproval copy of digital video apparatus. This method carries out the leg of the watermark information directly at the place where an image waveform etc. are not conspicuousor embeds watermark information at the specific frequency component of the frequency conversion information on the HARASHIN item. By giving information that a copy is possible / improper to this watermarkspecification of C etc. is attained only a copy good and reproduction freely.
[0006]
[Problem(s) to be Solved by the Invention]Howeverwith the conventional copy control method using CCIwhen rewriting CCI by receiver apparatus from "10" (a copy is possible once) to "11" (a copy is impossible)it becomes possible comparatively simply by operation in which it is 2 bits to rewrite "10" to "00" (a copy is freely possible). For this reasonthere is a problem that a disapproval copy is easy.
[0007]Since watermark information is distributed by the comparatively wide range concerning the image and sound in main datathe method of using a watermark cannot rewrite this easily by receiver apparatus. If it is going to rewrite this by user levelsit must have a quite large-scale circuit. For this reasonit is effective in that a disapproval copy is prevented rather than CCI. Howeversince rewriting of a watermark cannot be performed simplyit cannot take easily the mode of rewriting a flag like [at the time of using CCI conversely]and permitting a copy only once.
[0008]This invention was made in view of such a problemand an object of an invention is to provide the digital copy control method that the digital copy which is not permitted can be prevented more effectivelyand the device using itmaking possible the mode which restricts a copy.
[0009]
[Means for Solving the Problem]A digital copy control method concerning this inventionVia an interface which two or more digital equipment is

connected via a busand performs authenticating processing mutually among these digital equipment and with which transmission and reception of digital data are performed only between attested apparatusFrom transmitting side apparatusface transmitting digital data from a digital recording medium to receiver apparatusand transmitting side apparatus and receiver apparatusSo that a disapproval copy may be prevented based on the contents of copy management information for copy restrictions included in said digital dataIn what performs reproduction of the transmitting side apparatus concerned and receiver apparatusand restriction of recording operation of operation<TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>Said copy management information which shows a copy restriction level is added to portions other than an image and/or a sound among main data recorded on said digital recording mediumAdd electronic watermark information to portions of an image and/or a sound among said main dataand. The justification of a digital recording medium which adds error information of a specific pattern to record data after adding an error correction code to said main data intentionallyand is reproduced by said transmitting side apparatus by existence of said copy management informationelectronic watermark informationand error information of a specific pattern. It identifiesand only data of a just disk performs the playbackand only suitable data is recorded.
[0010]To said main data of a digital recording medium concerning this invention. Copy management information rewritten so that said copy restriction level may be strengthened by a digital copywhen a copy restriction level is shown in portions other than an image and/or a sound and it restricts a digital copy is includedIn the state in which read-out outside is possibleit is included in portions other than an image and/or a sound by electronic watermark information which is not rewritten by digital copyeitherand besides said main dataIt is added by medium mark which is not read outside and these copy management informationelectronic watermark informationand a medium markIt is constituted so that medium reproduction management and medium copy management by the side of a maker of said main data to mean may be made with combination of the contents of these three kinds of information.
[0011]This invention is characterized by a digital recording medium manufacturing device comprising the followingin order to restrict a copy to original dataa watermark information addition means which adds electronic watermark information which does not spoil the feature to original dataand.
A copy-management-information addition means which adds copy management information.
An error correction code creating means which generates and adds an error correction code from main data in which said electronic watermark information and copy management information were added to original data.
An error addition means which adds an error of a specific pattern to data in which an error correction code was added by this error correction code creating means as a medium mark.

[0012]Via an interface which performs authenticating processing mutually among two or more digital equipment connected via a bus and with which transmission and reception of digital data are performed only between attested apparatusDigital playback equipment concerning this invention used as said transmitting side apparatus of a system which transmits digital data to receiver apparatus from transmitting side apparatusA reading means which reads record data from a digital recording mediumand an error detection correcting means which carries out detection correction of the error of read-out data read by this reading meansA specific pattern detection means to detect that an error detected by this error detection correcting means is a specific patternAn output means which outputs data by which the error correction was carried out by said error correction means to said bus with a gestalt of digital information suitable for specification of said interfaceA <DP N=0005><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>copy-management-information judging means which identifies and judges copy management information for restricting a digital copy contained in said data by which the error correction was carried outHave an electronic-watermark-information judging means which identifies and judges electronic watermark information which shows a copy restriction level from said data by which the error correction was carried outand said digital recording medium judges an original medium or a copy medium based on a detection result of an error detection means of said specific patternThis decision result and a decision result in said copy-management-information judging means and said electronic-watermark-information judging means were made to perform execution or prohibition of reproduction motion.
[0013]In one concrete mode of this inventionas information currently

recorded into a recording mediumSaid copy management information can be one-generation copied [a copy freelancer and]or has one state of three kinds of copy restriction levels of copy prohibitionSaid electronic watermark information takes either a copy freelancer or two kinds of copy restriction levels of copy prohibitionAs a state whether it is related with an error of said added specific pattern or there is nothing was taken and it was able to be judged whether it is the disk regularly recorded in combination of these each signalit enabled it to identify a regular disk.
[0014]In other concrete modes of this inventionan error of a specific pattern is detected by said specific pattern detection meansReproduction motion is performedwhen it is judged with an one-generation copy being possible by a copy-management-information judging means and is judged with electronic watermark information being copy prohibition in an electronic-watermark-information judging means.
[0015]In a concrete mode of further others of this inventionby a case where an error of a specific pattern is detected by said specific pattern detection meansand a decision result of said copy-management-information judging means and said electronic-watermark-information judging meansWhen it is contents which conflict except for a case where an one-generation copy of copy management information is possibleand electronic watermark information serves as copy prohibitionOr when an error of a specific pattern is detected by said specific pattern error detection meansand when said electronic watermark information is not able to be detectedit does not reproduce.
[0016]In a concrete mode of further others of this inventionwhen an error of a specific pattern is not detected by said specific pattern error detection meansand when decision results of said copy-management-information judging means and said electronic-watermark-information judging means differit does not reproduce.
[0017]A digital recording device concerning this inventionVia an interface which performs authenticating processing mutually among two or more digital equipment connected via a bus and with which transmission and reception of digital data are performed only between attested apparatusIn a digital recording device used as said receiver apparatus of a system which transmits digital data to receiver apparatus from transmitting side apparatusA copy freelancer and said copy management information which an one-generation copy is possible or shows three kinds of copy restriction levels of copy prohibition are <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>added to portions other than an image and/or a soundand. An one-generation copy of copy management information which receives digital data in which a copy was possible into portions of an image and/or a soundor two kinds of electronic watermark information of copy prohibition were added to them and which was received and identified is possibleAnd when identified electronic watermark information is copy prohibitionelectronic watermark information is recorded as it isand rewrites and records only copy management information on copy prohibition.
[0018]According to this inventionthe justification of a digital recording medium is judged using three kinds of information. The 1st information is the copy management information which shows a copy restriction level contained in portions other than an image and a sound among main dataand when restricting a digital copyif copiedit will be rewritten so that a copy restriction level may be strengthened. The 2nd information is the electronic watermark information which is similarly included in portions of an image and a sound among main dataand shows a copy restriction leveleven if the digital copy of this information is carried outit is not rewrittenand rewriting is very difficult. The 3rd information is the error information (it is hereafter called a medium mark) of a specific pattern intentionally added to data after an error correctionand since it is added out of main datathis information is not included in main data reproduced from a recording mediumbut if a digital copy is carried outit will disappear.
[0019]Thussince three information has character differentrespectivelyit can be judged in detail whether it is that to which a digital recording medium was justly copied by state of these three information. That isfirstsince it will disappear if the digital copy of the medium mark is carried out onceit can judge an original medium or a copy medium by existence of a medium mark. Although both copy management information and electronic watermark information show a copy restriction levelIn the case of a medium with a good digital copyfreely copy management information and electronic watermark informationOnly all of combination which shows copy C freely are effectiveand since others may have been rewritten without passing through processing that copy management information is regulara medium by which a medium mark is not detected can be recognized to be a medium which is not just. When copy management

information and electronic watermark information must show a copy restriction level when [both] it permits a copy under a certain restrictionand either shows copy C freelythis is also a medium which is not just. When each of copy management information and electronic watermark information shows a predetermined copy restriction levelonly copy management information is rewritten by copybut. Even if it is intentionally rewritten at this time so that copy management information may fall or maintain a copy restriction level as isthis is recognized by disappearance of a medium mark and it can judge with it being a medium which is not just.
[0020]Since transmitting side apparatus forbids reproduction of digital data when it is presumed by transmitting side apparatus as a result of such a judgment that it is a medium which is not justthe medium can perform neither reproduction nor recordbuttherebycan <DP N=0006><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>prevent a disapproval copy effectively. Since digital data is transmitted to attested receiver apparatus so that it may become possible [only reproduction] good [record reproduction] according to the copy restriction level when it has been recognized as transmitting side apparatus being a just mediuma digital copy under restricted conditions also becomes possible.
[0021]Also when it is possible to carry out digital recording via an analog signal between attested apparatusAttest only between these-attested apparatus and ******** electronic authentication signature data is recorded with digital data contentsIf reproduction of data contents is permitted only when this attestation is materialized further in addition to the recognition technique mentioned abovea disapproval copy of the data contents themselves can be prevented more certainly.
[0022]
[Embodiment of the Invention]Hereafterthe desirable embodiment of this invention is described with reference to drawings. <A HREF="JP-A-2000-48478.files/000003.gif">Drawing 1 </A>is a block diagram showing the composition of the digital data transmission and reception system concerning one example of this invention. DVD player 1 which is transmitting side apparatusand the display device 2 and DVD recorder 3 which are receiver apparatus are mutually connected via each interfaces 45and 6 and bus 7 based on IEEE1394 specification. DVD player 1 transmits the digital data produced by reproducing DVD8 on which the image and the music content used as transmitting sauce were recorded to the display 2 and the recorder 3 via the bus 7. The recorder 3 records on DVD9 the digital data which was restricted when it was digital data in which the digital copy is permittedand was received.
[0023]The player 1 performs [whether it is apparatus by which these each apparatus operates between the display device 2 and the recorder 3 as a contents creator's intentionand] mutual recognition processing in advance of reproduction of DVD8. For examplesince there is no recording functionfor example in the display device 2the full attestation which used the public key is materialized between the players 1. In this casedata will be transmitted if the contents to which record is forbidden are also renewable. Between the player 1 and the recorder 3the attestation with restriction which used the common key is materialized. In this casedata transfer only of the contents for which record and reproduction are also good is carried out. The data on the bus 7 is enciphered so that data transfer may become effective only between the attested apparatus.
[0024]Whether the player 1 is a medium with just DVD8 which it is going to reproduce. It verifies by three kinds of information currently recorded on DVD8i.e.CCI(copy management information)the watermark (electronic watermark information)and a media mark (medium mark: error information of a specific pattern).
[0025]<A HREF="JP-A-2000-48478.files/000004.gif">Drawing 2 </A>is a block diagram showing the composition of the original recording manufacturing device which produces the original recording of DVD in which these information was added. The HARASHIN item which should be recorded is the watermark adjunct 11and <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>embeds a watermark at the portion into which the HARASHIN item is not conspicuousfor examplethe big portion of luminance difference with a masking effectetc. It may be made for a watermark to embed the HARASHIN item in the specific frequency of the signal which carried out the Fourier transform. Although compression encoding of the signal with which the watermark was embedded is carried out by the encoder 12it is either of the processes so farand 2-bit CCI which production persons mean is added by the CCI addition means which an inside does not illustrate. HereCCI is added with the encoder 12. Nextafter ID and an error detection code are added by the ID/EDC adjunct 13an error correction code is added in the ECC generation part 14. The data in which the error correction code was added can bear about 1% of reading errorfor example. Herethe error information

of a specific pattern is added as a media mark by the error addition means 15 to such an extent that such an error rate is not exceeded. That isa bit error is produced intentionally. The pattern or the pattern on a frequency axis on a time-axis may be sufficient as a media mark. The data in which the media mark was added is the eight-to-fourteen modulation part 16and 8->16 (DVD) or 8->14 (CD) abnormal conditions of it are carried outand it is recorded on the original recording disk 18 by the record driver 17. DVD produced by this original recording 18 serves as the original version.
[0026]<A HREF="JP-A-2000-48478.files/000005.gif">Drawing 3 </A>is a block diagram showing the details of the player 1 of <A HREF="JP-A-2000-48478.files/000003.gif">drawing 1</A>. After the record data recorded on DVD8 being read by the read head 21 and getting over by the EFM demodulation section 22error correction processing is made by the ECC demodulation section 23. The media mark detection part 24 asks for the tendency of the error pattern in the ECC demodulation section 23 by correlation operation etc.and when the error has occurred by the specific pattern decided beforehandit judges with those with a media mark. The output from the media mark detection part 24 is supplied to the output control part 26. The data to which it restored by the ECC demodulation section 23 is supplied to the decoder 25 through the CCI judgment part 28 and the watermark judgment part 27. The watermark judgment part 27 and the CCI judgment part 28 judge the watermark and CCI which were extractedrespectivelyand output a decision result to the output control part 26. It may be made to judge in not in signal decoding processing but the frontor the back depending on recording methodssuch as a watermark. The output control part 26 from the decision result of the detect output of the media mark detection part 24the watermark judgment part 27and the CCI judgment part 28. When it is judged that data communications are possibleit controls to supply to I/F29 the main data which contains a watermark and CCI from the decoder 25 and which should be transmitted. In forbidding reproduction of a playerit controls the reproduction control part 31 if needed. And when data is supplied to I/F29the main data which should be transmitted is changed into the fixed bit rate based on IEEE1394and is outputted on the bus 7.
[0027]On the other hand<DP N=0007><TXF FR=0001 HE=250 WI=080 LX=0200 LY=0300>when main data has been transmittedsince the recorder 3 is in the state which can be copiedit carries out the digital copy of thisbut. When copy C is shown only under restriction with the watermark and CCI which are contained in main datait rewrites so that a restriction level may go up CCI simultaneously with a copy.
[0028]<A HREF="JP-A-2000-48478.files/000006.gif">Drawing 4 </A>is a table showing good/failure of the media mark and watermark which the output control part 26 judgesCCI and reproductionand record. Since the media mark is not included in the main data which should be transmitted as mentioned aboveit does not exist in a copy disk. Naturally it is not contained in the old disk of DVD or CD. For this reasonthe disk with which a media mark exists can be judged to be an original diskand the disk not existing can be judged to be a copy disk or the old disk.
[0029]A watermark is set as "11"when restricting "00" and a copyin permitting a copy freely. CCI presupposes freely that a copy is impossible at a copy good and "11" only once by "00" a copy good and "10." When a watermark does not existsince it is the old diskthe combination of those with a media mark is contradictory without a watermark. Thereforeit is considered as invalidity (it is not just) irrespective of the pattern of CCI in this case. When there are not both a media mark and a watermarksince it is the old disklet only copy C (10) and playback be C (11) only copy C (00) and once freely according to CCI.
[0030]When both a watermark and CCI are "00"since a copy is possiblerecord and reproduction are freely permitted irrespective of the existence of a media mark. Howeversince inconsistency arises when a watermark is [CCI] "10" or "11" in "00"it thinks that intentional bit manipulation was made and is considered as the disk which is not just.
[0031]Since it is a copy with restriction when a watermark is "11"CCI is set to "10" or "11." Thereforewhen CCI is "00"it is dealt with with the disk which is not just. CCI judges with the disk which rewrote CCI intentionally and carried out it and which is not justwhen there is a media markand only 1 time is effective and there issince it must be an original disk at the time of copy C (10). [no] Since it is copy prohibition when CCI is "11"only reproduction is made good.
[0032]Since neither playback nor record is permitted when it judges that DVD8 is a disk which is not just by the above judgmentthe player 1 does not transmit main data to the display device 2 and the recorder 3. When only reproduction is judged to be goodmain data is transmitted to the display device 2

and the recorder 3but since the data has CCI only with reproductionthe recorder 3 which is the composition that attestation can be received does not perform recording operation.
[0033]The <TXF FR=0002 HE=250 WI=080 LX=1100 LY=0300>view of this reproduction and propriety control of record agrees not only to the digital data transmission system shown in the example but to the system of the digital reproduction and the recording device by transmission using the analog signal which existed from the former well. For examplein that casesince a watermark is put in when an analog input is used as an input source as shown in <A HREF="JP-A-2000-48478.files/000006.gif">drawing 4</A>media mark nothing and CCI can be processed like this inventionif it considers that it applies to a watermark. Since a next watermark and CCI can also be given satisfactorily at all if it regards as those with a media mark with the registered digital broadcast wave being receivable in inputting a digital broadcast waveit can process like this invention.
[0034]Two or more digital equipment which was explained previously is connected via a busEven if it is a digital data transmission system through the interface with which authenticating processing is mutually performed among these digital equipmentand transmission and reception of digital data are performed only between the attested apparatusIf recorded on a just mediumthat sound and/or the contents of reproduction of an image can be outputted as an analog signaland a possibility that digital recording will be again carried out to another recording medium about this output using the apparatus or the illegal apparatus of not attesting other than the attested apparatus remains. Such a recording medium in an attestation apparatus system. as the medium of the old system without a watermark or a media mark -- not recognizingif it does not obtain but it is recorded that a copy freelancer or an one-generation copy of the CCI is still more nearly possibleWhen this medium is carried in between attestation apparatus systems once againnot to mention reproductionbased on CCI for which an one-generation copy is gooda copy medium will be again created with the attestation apparatus system itselfand a just medium may be made from the medium which is not just. Of courseforbidding an analog output entirely cannot be carried outand also giving encryption (encryption) to an analog output and including a decryption circuit in all the image display devices which are in all reproduction side apparatusfor example in the world cannot be realized in practiceeither.
[0035]What is necessary is just to constitute so that additional use of the electronic authentication signature data which can be recognized only between these attestation apparatus systems to the record and/or reproduction motion in the attested apparatus may be carried out in order to prevent from reproducing the medium which was created using such non-attesting apparatus and which is not just by the attested apparatus. Therebybetween attestation apparatus systemswhether the record data of that medium is what was justly recorded within the attestation apparatus system can check by this electronic authentication signatureand it becomes possible to control execution of reproduction and/or recording operation on it. Thereforeeven if it is going to reproduce the medium data which was recorded using non-attesting apparatus and which is not just by the apparatus of either of the attestation apparatus systemsThe electronic authentication signature which should be performed between attestation apparatus systems does not existor the authentication result of an electronic authentication signature becomes abortiveand <DP N=0008><TXF FR=0001 HE=170 WI=080 LX=0200 LY=0300>use of the medium which is not just can be prevented by being made not to perform reproduction motion in this case.
[0036]Although various data encryption methods can be used about generation and attestation of an electronic authentication signaturethe example using what applied for examplethe public-key-encryption-ized method here is explained. A RSA (RivestShamirAdleman) code typical as a public-key-encryption-ized method sets the antecedent basis of safety to the difficulty of a large number of factorization into prime factorsand performs encryption/decoding processing by calculation of a exponentiation surplus. An enciphering procedure is expressed with "the C=E(M) = (e-th power of M) surplus n"and a decryption procedure is expressed with "M=D(C) = (d-th power of C) surplus n." HereM is a plaintext and C is a cryptogram. enand the decryption key of an enciphering key are d and nthe enciphering key e and the common key n are exhibitedand the decryption key d presupposes that it is secret. A decision of the key edand n is made in the following procedure. (1) Choose the two big prime numbers p and q arbitrarilyand consider it as n=pq. The least common multiple L of (2)(p-1)and (q-1) is calculatedit is as relatively prime as L and the arbitrary

integers e smaller than L are searched for. (3) Ask for d which fills the ed=1 surplus L. In this wayas for the selected value edand nsurplus (ed ** of M) n=Mis materialized to all the plaintexts M. Although a decoder has to know the decryption key d to decode the cryptogram Cit is necessary to get to know the secret prime numbers p and q for that purposeto calculate "-1st power surplus L of d=e" from the least common multiple L of (p-1) and (q-1)and the public key eand to ask for the secret key d. Since the public key n is a product of the prime numbers p and qit does not become a code for the integer which is a grade which the public key n can factorize into prime factor easily. Thenp and q are usually made into a 100-figure each (decimal number) gradeand the public key n is made into about 200 figures. If it carries out like thiseven if it uses a 1000-MIPS electronic computerit will be this calculation to factorization into prime factors for millions yearsand the decipherment is substantially impossible.
[0037]Operation of the apparatus in a concrete attestation apparatus system is explained. The common key n is first memorized beforehand by each apparatus in an attestation apparatus system. <TXF FR=0002 HE=110 WI=080 LX=1100 LY=0300>When writing in these apparatus through the data contents which should be recordedwithin apparatusThe contents which combined apparatus recognition ID of self and peculiar ID of contents which should be recorded are enciphered with the enciphering key e currently exhibitedand it creates as data of an electronic authentication signatureand records on a medium with the data contents which should record this. Only when it decrypts using a common key and the secret decryption key of external disclosureand it confirms apparatus ID and data content IDin operating this medium by the apparatus of either of the attestation apparatus systemsand being just is admitedit controls to reproduce this. If this data medium is recorded by non-attesting apparatus. [whether there is any data of an electronic authentication signatureand] Or it becomes a thing (the specific encryption which is common between attestation apparatus systems is not made) which cannot be decryptedand it hasand this is not accepted to be a just mediumand such data contents are not reproduced.
[0038]
[Effect of the Invention]As stated aboveaccording to this inventionby combining the information on three kinds of different characterIt can be judged clearly whether it is what has a just digital recording mediumand the effect that the digital copy which is not just can be prevented more effectively is done somaking possible the mode which restricts a copy by this.
</SDO>
<HR><B>DESCRIPTION OF DRAWINGS</B>
<HR><SDO EDJ><TXF FR=0003 HE=060 WI=080 LX=1100 LY=1400>[Brief Description of the Drawings]
<A HREF="JP-A-2000-48478.files/000003.gif">[Drawing 1]</A>It is a block diagram of the digital data transmission system concerning one example of this invention.
<A HREF="JP-A-2000-48478.files/000004.gif">[Drawing 2]</A>It is a block diagram of the original recording manufacturing device of the disk which applied this invention.
<A HREF="JP-A-2000-48478.files/000005.gif">[Drawing 3]</A>It is a detailed block diagram of the player of the system of <A HREF="JP-A-2000-48478.files/000003.gif">drawing 1</A>.
<A HREF="JP-A-2000-48478.files/000006.gif">[Drawing 4]</A>It is a figure showing the good/improper correspondence relation between three kinds of informationrecordand reproduction used by this invention.
[Description of Notations]
1 [-- An interface7 / -- Bus.] -- A player2 -- A display device3 -- A recorder456
</SDO>
<HR></BODY></HTML>